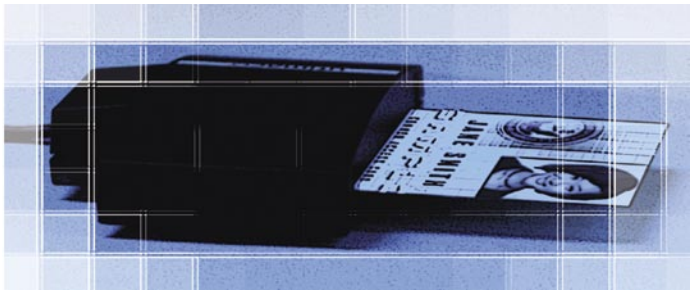
Cryptographic Log-on ... Coming Soon

By James Mauck



Cryptographic log-on (CLO) is a process that uses the Common Access Card (CAC) and embedded Public Key Infrastructure (PKI) certificates to authenticate a user's identification to a workstation and network. It replaces the username and passwords used today for identifying and authenticating users. To log-on cryptographically to a CLO-enabled workstation, users simply insert their CAC into their workstation's CAC reader and provide their six to eight-digit Personal Identification Number (PIN).

The Secretary of Defense has embraced public key cryptography as a critical component of Defense-in-Depth and contributor to the overall Department of Defense (DoD) information assurance (IA) strategy for protecting its information and networks. DoD Instruction 8520.2, "Public Key Infrastructure and Public Key Enabling" (available on the DON CIO Web site at http://www.doncio.navy.mil) establishes the requirements for PK-enabling all e-mail, private Web servers and networks.

Today, users typically identify themselves to the network with their username. The network authentication process requires that users prove they are actually who they claim to be. Authentication evidence can be provided by something unique, such as a password, CAC, PKI-certificate or biometric fingerprint. Providing more than one form of evidence increases the strength and assurance of the user's identity.

Cryptographic log-on uses "two-factor" or strong authentication and provides a higher level of assurance than traditional passwords. Multiple recent network defense exercises have shown that passwords are becoming a weak link because they are easy to share, not hard to gather through social engineering efforts and are easy to break using advanced password cracking tools. CLO mitigates many of the risks associated with passwords because to masquerade as a user, a potential attacker must physically have control of a user's CAC and know his or her PIN.

Cryptographic log-on is the first step toward a future single (or reduced) sign-on environment in which we will need fewer passwords — passwords we won't have to manage, remember, change every 90 days or call the help desk to have reset. Expanded use of PK-enabled portals and Web servers will further eliminate the need for traditional username and password authentication.

By using the PKI credentials you provided during the CLO process at the beginning of your network session, PK-enabled portals and Web servers will transparently perform the authentication and access control functions on your behalf. Insert your CAC, enter your PIN, and you are done. The benefit of single (or reduced) sign-on is multiplied when a compromise occurs because by revoking a user's PKI certificate, a user's access is terminated in any environment relying on that certificate for access control.

The Navy Marine Corps Intranet (NMCI) will lead the way within the Department of the Navy for CLO enablement. Within the NMCI there is already a small pilot group successfully using CLO. Larger scale, capability proof-of-concepts will commence in spring 2006 for the Navy at the Space and Naval Warfare Systems Command in San Diego, Calif., and for the Marine Corps at Quantico, Va. NMCI-wide CLO enablement will begin upon successful completion of those capability demonstrations.

Parallel efforts are underway within the Department's non-NMCI business and tactical networks to ensure they are afforded the same robust security enhancements provided by CLO. The infrastructure upgrades and improvements required to support CLO are being implemented enterprise-wide to support the Marine Corps Enterprise Network (MCEN), the Navy's ONE-NET and Integrated Shipboard Network System (ISNS) networks afloat.

You can prepare now for the change. Verify that you have your CAC, that it has all of the required certificates and that you know your PIN. If your CAC is locked or is missing certificates, visit your local RAPIDS (Real-time Automated Personnel Identification System) site or find the nearest site by linking to http://www.dmdc.osd.mil/rsl/.

If you do not already do so, keep your CAC with you at all times. Once you are enabled for CLO, you will not be able to use your computer without your CAC. Also, removing your CAC will lock your workstation and prevent anyone from using it while you are logged in.

Become familiar with using your CAC for signing and encrypting appropriate e-mail or when accessing PK-enabled Web sites. Review the PKI and CAC training modules on NMCI e-Learning available from your NMCI workstation by going to http://training/mgen-img/library/html/crs_display.htm/, select the "Catalog" tab and type in PKI. For PKI/CAC user information link to http://www.nmci-isf.com/userinfo.asp/.

James Mauck is a contractor supporting the DON CIO Information Assurance Team.

CHIPS